Auteur: Xander Bordeaux en Ruud Wissenburg zijn IT-onderzoekers bij de Algemene Rekenkamer. Zij zijn bereikbaar via voorlichting@rekenkamer.nl

De Algemene Rekenkamer onderzoekt of de rijksoverheid publiek geld zinnig, zuinig en zorgvuldig uitgeeft. Onze wettelijke taak is het controleren van de inkomsten en uitgaven van het Rijk en hierover rapporteren wij één keer per jaar aan het parlement op Verantwoordingsdag (derde woensdag in mei). Op basis van ons oordeel kan het parlement besluiten of hij decharge verleent aan het kabinet. Daarnaast rapporteren we afzonderlijke onderzoeken aan het parlement zodat Kamerleden kunnen bepalen of het beleid van een minister doeltreffend is. Voor meer informatie: www.rekenkamer.nl en bekijk ons dashboard Doelen & Resultaten op blikopnederland.rekenkamer.nl

Het Rijk in de cloud

Digitale soevereiniteit onder druk

Dit artikel is gebaseerd op het onderzoek Het Rijk in de cloud – Donkere wolken pakken samen, uitgevoerd door de Algemene Rekenkamer over het cloudgebruik bij de rijksoverheid. De onderzoeksresultaten zijn in 2025 gepubliceerd waarbij de nadruk ligt op kansen, risico's en – bij de toetsing – op de bevindingen rond digitale soevereiniteit, continuïteit en gegevensbescherming. De auteurs van dit artikel hebben beiden aan dit onderzoek meegewerkt.

Cloud als strategische keuze, niet slechts een technische

De migratie van applicaties van de rijksoverheid naar de cloud is geen IT-project, maar een strategische herpositionering van: digitale macht, afhankelijkheden en verantwoordelijkheden. Het rapport Het Rijk in de cloud – Donkere wolken pakken samen (1) beschrijft hoe de rijksoverheid in relatief korte tijd grootschalig gebruik is gaan maken van public cloud-diensten, terwijl de governance, risicobeheersing en strategische sturing daar niet in gelijke mate in zijn meegegroeid.

Voor wie zich bezighoudt met informatiebeveiliging en digitale weerbaarheid is dit rapport bijzonder relevant. Het legt bloot dat cloudgebruik niet alleen draait om kosten, innovatie en efficiëntie, maar vooral om fundamentele vragen rond soevereiniteit, controle, continuïteit en bescherming van publieke waarden. Vragen die niet alleen bij (public) cloud gesteld moeten worden maar eigenlijk bij (overheids)uitbesteding in het algemeen.

Het onderzoek richt zich op de praktische invulling van het rijksbrede cloudbeleid (herzien in 2022) en specifiek op de mate waarin ministeries zicht hebben op hun cloudgebruik en bijkomende risico's. Daarnaast zijn in het onderzoek drie belangrijke public cloud contracten onderzocht op de borging van drie kernprincipes: digitale soevereiniteit, continuïteit van dienstverlening en gegevensbescherming.

De conclusies zijn zorgwekkend: de rijksoverheid heeft beperkt zicht op zijn cloudgebruik, maakt onvoldoende strategische risicoafwegingen en waarborgt in het drietal onderzochte contracten de kernprincipes onvoldoende.

Vanuit beveiligingsperspectief is vooral de bevinding rond soevereiniteit fundamenteel: het Rijk heeft zich afhankelijk gemaakt van een beperkt aantal, grotendeels Amerikaanse hyperscalers, zonder altijd helder te hebben welke structurele risico's dit meebrengt. Voor velen was dit wellicht niet een verrassende uitkomst. Echter, het onderzoek heeft wel mede de maatschappelijke discussie aangejaagd en voor grotere politieke interesse gezorgd. Interesse die zich niet meer beperkte tot de technische maar vooral ging over de strategische afwegingen.

De context: waarom dit onderzoek noodzakelijk was

De cloud push

In ons onderzoek beschrijven wij hoe IT-ontwikkelingen de rijksoverheid richting cloud duwen. Leveranciers bieden hun producten steeds vaker uitsluitend als cloudoplossing aan. Microsoft 365 is daarvan het meest duidelijke voorbeeld: klassieke on-premise versies verdwijnen of worden niet langer doorontwikkeld met nieuwe functionaliteit. Voor ministeries ontstaat hierdoor een praktisch dilemma: vasthouden aan verouderende systemen zonder innovatie of meegaan in cloudmigratie met nieuwe afhankelijkheden.
Vanuit beveiligingsoptiek is dit geen neutrale beweging. De keuze voor cloud is in veel gevallen geen vrije strategische afweging, maar een reactie op marktdynamiek. De onderhandelingspositie van individuele ministeries is daarmee per definitie beperkt.

Beleidsontwikkeling en onderzoeksaanpak

Tot 2022 was public cloud binnen de rijksoverheid niet toegestaan. Toch hadden verschillende ministeries al eigen beleid ontwikkeld waarin public cloud onder voorwaarden werd geaccepteerd. De behoefte was urgent en de druk vanuit leveranciers groot. In 2022 werd het rijksbrede cloudbeleid herzien: public cloud werd toegestaan, mits onder strikte voorwaarden en niet voor zeer vertrouwelijke informatie. In het onderzoek van de Algemene Rekenkamer hebben wij twee voorwaarden uit het beleid getoetst; ministeries moeten zicht hebben op hun eigen cloudgebruik en er moeten risicoafwegingen zijn gemaakt.

Daarna hebben wij uit de inventarisatie van het cloudgebruik drie belangrijke cloudcontracten onderzocht op maatregelen die risico's beheersen op het gebied van: soevereiniteit, continuïteit en gegevensbescherming.

De vraag in het onderzoek was eenvoudig maar fundamenteel: "Wordt aan de geselecteerde voorwaarden voldaan en worden de drie onderzochte risico's voldoende afgedekt?" De bevindingen moesten het cloudgebruik demystificeren en met de praktijkervaring input geven voor een herziene versie van het overheidsbeleid dat in 2025 stond gepland.

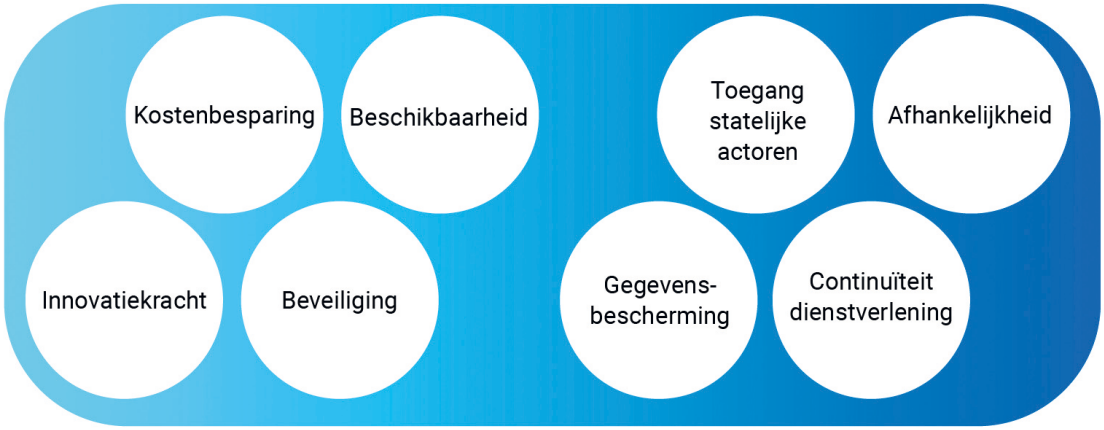
Kansen van cloud: realiteit en relativering

In het onderzoek wilden we niet alleen de risico's benoemen maar ook ingaan op kansen bij cloudgebruik. Vanuit een securityperspectief verdienen deze kansen echter enige nuance.

Kostenbesparing en schaalbaarheid

Cloudtechnologie maakt elasticiteit mogelijk: in theorie kan capaciteit eenvoudig naar behoefte worden opgeschaald of afgeschaald. Dit voorkomt investeringen in ongebruikte

Kansen en risico's van cloud; afhankelijk van de wens en cloudvorm kunnen kansen risico's zijn en vice versa



hardware. Maar de praktijk is complexer:

- licentiemodellen zijn vaak ingewikkeld;
- pay-per-use kan bij verkeerd gebruik tot kostenexplosies leiden;
- cloudtransformatie vereist nieuwe expertise en governance;
- schaalbaarheid is sterk afhankelijk van de mogelijkheden die de applicatie architectuur en infrastructuur biedt (pas bij cloud-native goed mogelijk).

Zonder volwassen cloudontwikkelomgeving en configuratiebeheer is kostenbesparing geen vanzelfsprekendheid.

Beschikbaarheid en redundantie

De grote cloudproviders bieden hoge beschikbaarheidseisen en een geografisch verspreide infrastructuur aan. Vanuit continuïteitsperspectief is dit enorm aantrekkelijk. De drie grootste cloudproviders (hyperscalers) zijn Amerikaanse bedrijven die zo'n 65% van de wereldwijde cloudmarkt bezitten. Door het gebruik van hyperscalers worden echter nieuwe risico's geïntroduceerd:

- concentratie van overheidsdata bij slechts enkele aanbieders;
- systeemrisico's bij grootschalige verstoringen;
- geopolitieke afhankelijkheden.

Beschikbaarheid op microniveau (per applicatie) kan toenemen, terwijl risico's op macroniveau groeien.

Beveiliging en expertise

Hyperscalers investeren miljarden in cybersecurity. Zij beschikken over gespecialiseerde teams, geavanceerde monitoring en snelle patching. Voor veel ministeries overstijgt deze capaciteit de eigen mogelijkheden. Dat is een reëel voordeel. Maar er is een belangrijke paradox: hoe groter de concentratie van gevoelige data, hoe aantrekkelijker het doelwit. Een succesvolle aanval op een hyperscaler of een misconfiguratie in een gedeeld platform kan enorme impact hebben. Security op schaal vergroot ook de impact van falen op schaal. Dit heeft in de praktijk ook al geleid tot grote incidenten, dus is ook een realistisch risico.

Innovatiekracht

Cloud is de basis voor AI, data-analyse en moderne digitale dienstverlening. Zonder cloud dreigt technologische achterstand. Toch rijst de vraag: mag innovatie afhankelijk worden van niet-Europese technologiebedrijven die onder buitenlandse wetgeving vallen? Hier raakt innovatie direct aan soevereiniteit.

De kern: digitale soevereiniteit – meer dan datalocatie

Het rapport heeft digitale soevereiniteit gedefinieerd als het vermogen om autonoom te beslissen en handelen over essentiële digitale aspecten van economie, maatschappij en democratie. Dit begrip is in het onderzoek geconcretiseerd in normen over:

- inzicht in datalocatie;
- afspraken over overdracht buiten de EER;
- right-to-audit;
- interoperabiliteit;
- portabiliteit en exitstrategie.

Het publieke debat versmalt soevereiniteit vaak tot "data in Europa". Het rapport laat zien dat dit te simplistisch is. Estland en Oekraïne kozen er bewust voor om overheidsdata buiten hun eigen grondgebied op te slaan om bij oorlog staatscontinuïteit

te waarborgen. Soevereiniteit kan dus ook betekenen: spreiding van afhankelijkheden. De kernvraag is niet waar data fysiek staat, maar:

- wie kan toegang afdwingen?
- wie bepaalt de spelregels, welke wetgeving is van toepassing?
- kan de overheid overstappen?
- kan zij audits uitvoeren en onafhankelijk afspraken laten toetsen?

Het gaat dus niet alleen om fysieke locatie, maar ook om controleerbaarheid en handelingsvermogen.

Amerikaanse wetgeving: het structurele spanningsveld

Cruciale onderdelen van het soevereiniteitsvraagstuk zijn de Amerikaanse CLOUD Act en de FISA Sectie 702. Amerikaanse autoriteiten kunnen op basis van deze wetten data opvragen bij Amerikaanse cloudproviders, ook wanneer deze data in Europa is opgeslagen. Historisch zijn meerdere afspraken tussen de VS en Europa zoals Safe Harbor en het Privacy Shield door het Europese Hof nietig verklaard. Het huidige EU-US Data Privacy Framework moet nog zijn robuustheid bewijzen onder president Trump.
In de praktijk zouden dergelijke verzoeken vanuit de VS zelden zijn gedaan. Maar juridisch is de mogelijkheid aanwezig. Experts bevestigen dit beeld. Het risico is dus niet verwaarloosbaar of afwezig. Te meer omdat de Amerikaanse inlichtingendiensten volgens FISA helemaal geen gerechtelijk bevel meer nodig hebben om inzage in de data te krijgen. Voor staatsgevoelige data is het formele risico zeer relevant, ongeacht de frequentie.

De toetsing: harde cijfers en zorgelijke patronen

Ons onderzoek maakt zichtbaar hoe het cloudgebruik binnen de rijksoverheid zich in de praktijk heeft ontwikkeld. Cloud wordt inmiddels breed toegepast, maar tegelijkertijd zien we dat de governance rond cloudgebruik nog onvolwassen is. Vooral het ontbreken van overzicht, uniforme definities en structurele risicoafwegingen zijn aandachtspunten.

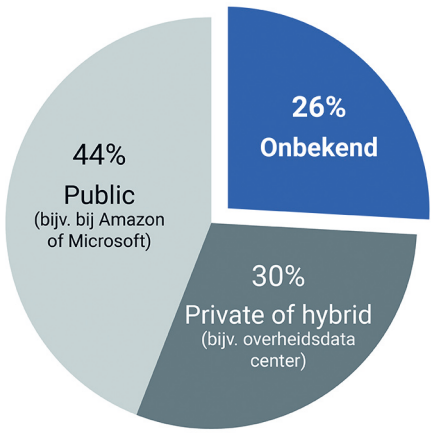
Gebrekkig overzicht

Uit het onderzoek blijkt dat de rijksoverheid in totaal 1.588 clouddiensten in zicht heeft. Deze zijn als volgt verdeeld:

- 700 public cloud-diensten (44%);
- 477 private of hybride cloud-diensten (30%);
- 411 diensten waarvan het type cloud onbekend is (26%).

Voor effectief risicomanagement is een dergelijk overzicht essentieel. Zonder inzicht in gebruikte diensten, leveranciers en dataopslaglocaties is het moeilijk om te sturen op compliance, beveiliging en continuïteit.

Bij een kwart van gerapporteerde clouddiensten is de vorm onbekend



Vanuit het perspectief van digitale soevereiniteit heeft dit directe consequenties. Wanneer niet duidelijk is in welke cloudomgeving data wordt verwerkt, is ook niet altijd bekend:

- waar de data fysiek is opgeslagen;
- welke wetgeving van toepassing kan zijn;
- en welke partijen potentieel toegang hebben tot de gegevens.

Dit maakt cloudgebruik niet alleen een technisch vraagstuk, maar vooral een governancevraagstuk.

Materieel public cloud: geen uniforme definitie

Van de 700 public clouddiensten zijn 126 diensten aangemerkt als 'materieel'. Dit zijn cloudtoepassingen die essentieel zijn voor de uitvoering van primaire overheidstaken, zoals belastinginning, communicatie met burgers of vitale informatievoorziening.
Ministeries hanteren verschillende definities voor het begrip 'materieel'. Sommige ministeries baseren dit uitsluitend op het belang voor primaire processen, terwijl andere aanvullende criteria gebruiken, zoals gevoeligheid van data of maatschappelijke impact bij uitval.
Het gevolg is een inconsistente classificatie van kritieke clouddiensten. Dit heeft meerdere gevolgen:

- risico's kunnen verschillend worden beoordeeld;
- rapportages tussen ministeries zijn moeilijk vergelijkbaar;
- centrale sturing op rijksniveau wordt bemoeilijkt.

Omdat het rijksbrede cloudbeleid vooral betrekking heeft op materieel public cloud-gebruik, leidt deze variatie in definities ertoe dat risico's niet altijd op dezelfde manier worden herkend of beheerst. Voor digitale soevereiniteit betekent dit dat de beoordeling van strategische afhankelijkheden en risico's versnipperd plaatsvindt.

Onvoldoende risicoafweging

Een opvallende bevinding uit het onderzoek betreft de wijze waarop risicoafwegingen plaatsvinden bij cloudgebruik.
Van de 126 materiële public cloud-diensten blijkt bij 84 diensten (67%) geen voorafgaande risicoafweging te zijn gemaakt. Met andere woorden: bij ongeveer twee derde van de kritieke cloudtoepassingen ontbreekt een gestructureerde analyse van de bijbehorende risico's. Een dergelijke risicoafweging zou minimaal moeten ingaan op drie kernprincipes die volgens de Rekenkamer centraal staan bij cloudgebruik door de overheid:

- digitale soevereiniteit – controle over data en systemen;
- continuïteit van dienstverlening – het vermogen om publieke diensten te blijven leveren;
- gegevensbescherming – het beschermen van vertrouwelijke gegevens van burgers en bedrijven.

Wanneer deze afweging niet expliciet plaatsvindt, blijven potentiële risico's buiten beeld en worden mitigerende maatregelen mogelijk niet genomen. Dit kan leiden tot situaties waarin:

- afhankelijkheden van leveranciers onvoldoende worden beheerst;
- continuïteitsrisico's niet zijn onderkend;
- of gevoelige gegevens onvoldoende beschermd zijn.

Contracttoetsing: waar soevereiniteit concreet wordt

Naast de kwantitatieve analyse van cloudgebruik zijn drie materiële public-cloudtoepassingen nader onderzocht.

Beperkte grip op contractuele afspraken

Een belangrijk aandachtspunt uit het onderzoek is de complexiteit van de contractuele structuur rond cloudleveranciers. Contractuele afspraken blijken vaak verspreid te zijn over meerdere documenten, zoals hoofdovereenkomsten, service-level agreements, aanvullende voorwaarden en technische bijlagen.
Daarbij spelen vaak verschillende partijen een rol, waaronder:

- primaire cloudleveranciers;
- integratie- of serviceproviders;
- en onderaannemers binnen de bredere leverancierskeketen.

Deze gelaagde structuur maakt het lastig om volledig overzicht te houden van alle contractuele verplichtingen en verantwoordelijkheden. Wij constateren dat hierdoor in de praktijk:

- niet altijd een volledig overzicht bestaat van contractuele afspraken;
- kennis over specifieke contractbepalingen beperkt kan zijn binnen ministeries;
- inzicht in de volledige leverancierskeketen niet altijd aanwezig is.

Voor digitale soevereiniteit is dit een belangrijk punt. Formeel kan controle over data, systemen en processen contractueel zijn vastgelegd, maar wanneer de contractstructuur complex en gefragmenteerd is, wordt praktische controle aanzienlijk moeilijker.

Exitstrategieën en afhankelijkheden

Een tweede belangrijk aandachtspunt betreft de mogelijkheid om van cloudleverancier te wisselen. In theorie vormt portabiliteit – het kunnen migreren van data en systemen – een belangrijk onderdeel van cloudcontracten. In de praktijk blijkt dit echter complex. Bij langdurig gebruik van specifieke cloudplatformen kunnen organisaties afhankelijk worden van de technologie en diensten van één leverancier.
Deze afhankelijkheid kan verschillende oorzaken hebben:

- integratie van cloudservices in bedrijfsprocessen;
- gebruik van leveranciersspecifieke functionaliteiten;
- technische en organisatorische migratiekosten.

Hierdoor ontstaat een situatie waarin overstappen naar een andere leverancier wel mogelijk is, maar in de praktijk ingrijpend, kostbaar en risicovol kan zijn. Voor digitale soevereiniteit betekent dit dat contractueel vastgelegde exit-mogelijkheden niet automatisch leiden tot feitelijke soevereiniteit. Zonder realistische migratiescenario's kan een exit-strategie vooral theoretisch van aard blijven.

Gegevensbescherming

Ook de bescherming van persoonsgegevens en andere gevoelige informatie vormt een belangrijk aandachtspunt bij cloudgebruik.
Wanneer meerdere partijen betrokken zijn bij de verwerking van gegevens, kan het lastig zijn om volledig inzicht te krijgen in:

- waar gegevens precies worden verwerkt;
- welke partijen toegang hebben;
- en hoe controle op naleving van afspraken plaatsvindt.

Voor organisaties die met gevoelige overheidsdata werken, betekent dit dat transparantie binnen de leverancierskeketen cruciaal is. Zonder voldoende inzicht in deze keten wordt het moeilijk om aantoonbaar te voldoen aan eisen rond gegevensbescherming, beveiliging en compliance.

Strategisch leveranciersmanagement: gemiste kans

De rijksoverheid behoort tot de grootste IT-afnemers van Nederland. Vanuit dat perspectief zou zij in principe over een aanzienlijke onderhandelingspositie moeten beschikken tegenover grote cloudleveranciers. Het onderzoek laat echter zien dat deze potentiële schaalvoordelen in de praktijk slechts beperkt worden benut. Cloudinkoop en contractbeheer vinden grotendeels plaats binnen afzonderlijke ministeries of uitvoeringsorganisaties. Hoewel er rijksbrede kaders bestaan voor cloudge-

bruik, is de toepassing ervan niet altijd uniform. Hierdoor ontstaat een situatie waarin verschillende onderdelen van het Rijk vergelijkbare diensten afnemen, maar niet altijd gezamenlijk optrekken richting leveranciers. Deze versnippering heeft directe gevolgen voor de strategische positie van de overheid in een markt die wordt gekenmerkt door sterke concentratie van aanbieders. Juist in een dergelijke marktsituatie is strategisch leveranciersmanagement op rijksniveau van belang. Gezamenlijke inkoop en gecoördineerde contractonderhandelingen kunnen helpen om sterker te sturen op voorwaarden rond bijvoorbeeld:

- audit- en controlemechanismen;
- locatie en bescherming van data;
- mogelijkheden voor migratie of beëindiging van diensten;
- juridische waarborgen rond toegang tot gegevens.

Effectief leveranciersmanagement vraagt niet alleen om technische en juridische expertise, maar ook om rijksbrede regie en coördinatie.

Cloud in geopolitiek perspectief: een structureel dilemma

Digitale infrastructuur is niet langer uitsluitend een technologische of economische kwestie, maar raakt in toenemende mate aan vraagstukken van soevereiniteit en nationale veiligheid. De internationale cloudmarkt wordt gedomineerd door een beperkt aantal grote technologiebedrijven. Veel van deze aanbieders zijn gevestigd buiten Europa. Voor overheden die in toenemende mate afhankelijk zijn van cloudplatformen voor hun digitale dienstverlening, betekent dit dat technologische keuzes ook geopolitieke implicaties kunnen hebben. Daarbij gaat het onder meer om:

- juridische afhankelijkheid, bijvoorbeeld door de mogelijke werking van buitenlandse wetgeving;
- politieke kwetsbaarheid, wanneer geopolitieke spanningen invloed hebben op toegang tot technologie of dienstverlening;
- strategische blootstelling, doordat vitale digitale infrastructuur buiten directe nationale invloedssfeer kan vallen.

Dergelijke afhankelijkheden zijn niet per definitie problematisch, maar moeten wel expliciet onderdeel zijn van de risicoafweging bij cloudgebruik.

Aanbevelingen: richting versterkte digitale soevereiniteit

In het rapport doen we aanbevelingen om de governance rond cloudgebruik binnen de rijksoverheid te versterken. De kern van deze aanbevelingen ligt niet zozeer in het beperken van cloudgebruik, maar in het professionaliseren van de besluitvorming, het toezicht en het leveranciersmanagement rondom cloudtoepassingen.

Uniformeer, concretiseer en handhaaf rijksbreed cloudbeleid
Een eerste aandachtspunt betreft het rijksbrede cloudbeleid. Hoewel er beleidskaders bestaan, blijken deze in de praktijk verschillend te worden geïnterpreteerd en toegepast door ministeries en uitvoeringsorganisaties. De Algemene Rekenkamer adviseert daarom om het beleid verder te uniformeren en te concretiseren, zodat duidelijker wordt welke eisen gelden bij het gebruik van cloudtechnologie.

Daarnaast pleiten we voor het structureel verplicht stellen van risicoafwegingen bij de inzet van cloudoplossingen. De eerder gesignaleerde lacunes – waarbij bij een aanzienlijk deel van de materiële public-clouddiensten geen expliciete risicoanalyse heeft plaatsgevonden – maken duidelijk dat een systematische benadering noodzakelijk is. Risicoafwegingen zouden daarbij niet alleen technische en operationele aspecten moeten omvatten, maar ook vraagstukken rond afhankelijkheden, gegevensbescherming en digitale soevereiniteit.

Ook de rol van de rijksoverheids CIO, de CIO-Rijk komt nadrukkelijk naar voren in de aanbevelingen. Volgens de Rekenkamer kan de centrale regiefunctie worden versterkt door duidelijkere kaders te stellen, de naleving van beleid beter te monitoren en waar nodig actief bij te sturen. Daarmee kan CIO-Rijk een belangrijkere rol spelen in het bewaken van rijksbrede belangen bij cloudgebruik.

Ga meer gezamenlijk optrekken om expertise te bundelen en sterker te staan
Verder wijzen we op het belang van gezamenlijke inkoop en contractbeheer. Door als rijksoverheid-CIO collectief op te treden richting cloudleveranciers kan de onderhandelingspositie worden versterkt en kunnen afspraken over bijvoorbeeld auditrechten, gegevensbescherming en migratiemogelijkheden beter worden geborgd.

Onderzoek nadrukkelijker alternatieve cloudleveranciers
In datzelfde kader adviseren we om nadrukkelijker te kijken naar Europese alternatieven en initiatieven die digitale soevereiniteit kunnen versterken. Hoewel dergelijke alternatieven momenteel nog niet altijd dezelfde schaal of functionaliteit bieden als de grote internationale cloudplatformen, kan strategische ondersteuning van Europese initiatieven bijdragen aan een meer evenwichtige markt.

Tot slot benadrukken we het belang van realistische exit-strategieën. De mogelijkheid om van leverancier te wisselen of cloudgebruik te beëindigen vormt een essentieel onderdeel van digitale soevereiniteit. In de praktijk blijkt echter dat dergelijke strategieën vaak onvoldoende zijn uitgewerkt of getest.

Wat CIO-Rijk, ministeries en SSO's moeten doen

Op 3 juli 2026 heeft de Ministerraad ingestemd met de herziening van het rijkscloudbeleid. Na onderzoeken van de Auditdienst Rijk, de Algemene Rekenkamer en vragen en moties uit de Tweede Kamer zijn aanbevelingen en adviezen meegenomen. Rijksorganisaties moeten bij het gebruik van publieke clouddiensten voortaan rekening houden met geopolitieke risico's en afhankelijkheid van één leverancier. De herziening 2026 is een update van het cloudbeleid uit 2022, heeft een breder bereik en bevat diverse aanscherpingen om de rijksoverheid te helpen om beter inzage in de risico's van cloudgebruik te krijgen.

Samen vormen deze elementen de basis voor een meer volwassen benadering van cloudgebruik binnen de rijksoverheid. Cloudtechnologie zal de komende jaren immers een centrale rol blijven spelen in de digitale infrastructuur van de overheid. Juist daarom is het van belang dat technologische innovatie gepaard gaat met sterke governance, transparante risicoafwegingen en strategische regie.

Slotbeschouwing: soevereiniteit als continu proces

Ons rapport schetst geen beeld van een overheid die lichtzinnig omgaat met cloudtechnologie. Wel maakt het duidelijk dat het gebruik van cloud binnen de rijksoverheid in belangrijke mate organisch en pragmatisch is gegroeid, terwijl een volledig geïntegreerd strategisch kader zich nog ontwikkelt.

Ministeries en uitvoeringsorganisaties hebben cloudoplossingen ingezet om digitalisering te versnellen en IT-voorzieningen te moderniseren. Deze ontwikkeling sluit aan bij bredere trends in zowel de publieke als private sector. Tegelijkertijd laat het onderzoek zien dat de governance rond cloudgebruik, met name op het gebied van: overzicht, risicobeheersing en rijksbrede coördinatie, nog niet overal dezelfde volwassenheid heeft bereikt.

Voor professionals in informatiebeveiliging ligt hier een belangrijke les. Digitale soevereiniteit is geen statische eigenschap, maar een continu proces van beheersing, heronderhandeling en strategische positionering. In een omgeving waarin technologie, marktdynamiek en geopolitieke verhoudingen voortdurend veranderen, vraagt soevereiniteit om blijvende aandacht voor governance, contractuele afspraken en afhankelijkheden.

De rijksoverheid staat daarmee voor een fundamentele opgave. Cloud kan worden benaderd als een efficiënt hulpmiddel voor IT-modernisering, maar kan ook worden beschouwd als strategische digitale infrastructuur die vraagt om expliciete regie en langetermijnbeleid.

De 'donkere wolken' waar de rapporttitel op wijst zijn daarmee niet zozeer een voorspelling, maar eerder een signaal. Dit onderstreept dat digitale soevereiniteit geen vanzelfsprekendheid is. Dit vraagt om actieve, gezamenlijke en strategische sturing. Zeker in een omgeving waarin overheidsprocessen steeds afhankelijker worden van cloudinfrastructuur.

Referenties

(1) https://www.rekenkamer.nl/documenten/2025/01/15/het-rijk-in-de-cloud